

## PATENT ABSTRACTS OF JAPAN

(11)Publication number : 2000-059604

(43)Date of publication of application : 25.02.2000

(51)Int.Cl.

H04N 1/387  
G06T 1/00  
G09C 5/00

(21)Application number : 10-226882

(71)Applicant : HITACHI LTD

(22)Date of filing : 11.08.1998

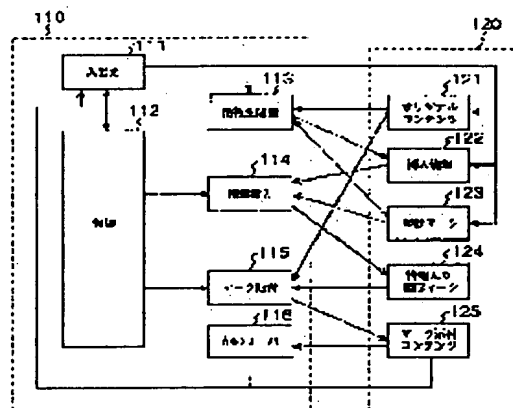
(72)Inventor : YOSHIURA YUTAKA  
SUZAKI SEIICHI  
NAGAI YASUHIKO  
SHINODA TAKASHI

## (54) METHOD FOR ATTACHING INFORMATION TO IMAGE AND METHOD FOR EXTRACTING INFORMATION FROM IMAGE

## (57)Abstract:

PROBLEM TO BE SOLVED: To attach information to image data while keeping the visibility of images indicated by the image data to a certain degree.

SOLUTION: An information insertion part 114 changes the image size of a graphic mark 123 so as to turn the number of vertical and horizontal pixels to  $32 \times n + a$  respectively. In this case, (a) is a decimal number indicated by the bit string of 5 bits of insertion information 122 to be buried and (n) is a numerical value for making  $32 \times n + a$  closest to the original image size (128, in this case) of the graphic mark 123. Also, the respective pixel values of the graphic mark 123 are changed so as to make the average value/contrast of the pixel values of the entire graphic mark 123 to  $32 \times n + a$ . In this case, (a) is the decimal number indicated by the bit string of 5 bits to be buried and (n) is the numerical value for making  $32 \times n + a$  closest to the average value/contrast of the original pixel values of the entire graphic mark 123.



## LEGAL STATUS

[Date of request for examination]

[Date of sending the examiner's decision of rejection]

[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]

[Date of final disposal for application]

[Patent number]

[Date of registration]

[Number of appeal against examiner's decision of rejection]

[Date of requesting appeal against examiner's decision of rejection]

[Date of extinction of right]

Copyright (C); 1998,2000 Japanese Patent Office

BEST AVAILABLE COPY

(19)日本国特許庁 (J P)

(12) 公 開 特 許 公 報 (A)

(11)特許出願公開番号

特開2000-59604

(P2000-59604A)

(43)公開日 平成12年2月25日(2000.2.25)

(51)Int.Cl.<sup>7</sup>

識別記号

F I

テマコード\*(参考)

H 0 4 N 1/387

H 0 4 N 1/387

5 B 0 5 7

G 0 6 T 1/00

G 0 9 C 5/00

5 C 0 7 6

G 0 9 C 5/00

G 0 6 F 15/66

B

審査請求 未請求 請求項の数19 O L (全 13 頁)

(21)出願番号

特願平10-226882

(22)出願日

平成10年8月11日(1998.8.11)

(71)出願人 000005108

株式会社日立製作所

東京都千代田区神田駿河台四丁目6番地

(72)発明者 吉浦 裕

神奈川県川崎市麻生区王禅寺1099番地 株

式会社日立製作所システム開発研究所内

(72)発明者 洲崎 誠一

神奈川県川崎市麻生区王禅寺1099番地 株

式会社日立製作所システム開発研究所内

(74)代理人 100087170

弁理士 富田 和子

最終頁に続く

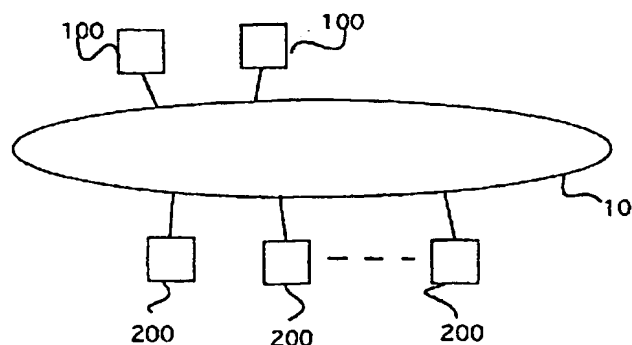
(54)【発明の名称】 画像への情報添付方法および画像からの情報抽出方法

(57)【要約】

【課題】 イメージデータが表す画像の視認性のある程度保ちながら、イメージデータに情報を添付する。

【解決手段】 情報挿入部114は、図形マーク123の画像サイズを、縦横それぞれの画素数が、 $32 \times n + a$ になるように変更する。ここで、 $a$ は、埋め込む挿入部122の5ビットのビット列が表す10進数であり、 $n$ は、 $32 \times n + a$ を、最も図形マーク123の元の画像サイズ(この場合は128)に近くする数値である。また、図形マーク123の各画素値を、その図形マーク123の全体の画素値の平均値/コントラストが $32 \times n + a$ になるように変更する。ここで、 $a$ は、埋め込む5ビットのビット列が表す10進数であり、 $n$ は、 $32 \times n + a$ を、図形マーク123全体の元の画素値の平均値/コントラストに最も近くする数値である。

図 1



**【特許請求の範囲】**

【請求項1】画像情報に非画像情報を添付する、画像への情報添付方法であって、

画像情報と当該画像情報に添付すべき非画像情報とを入力するステップと、

前記入力した画像情報を、当該画像情報が表す画像の特徴値が、前記入力した非画像情報の値と所定の規則とに応じて定まる値となるように変更するステップと、を有することを特徴とする画像への情報添付方法。

【請求項2】請求項1記載の画像への情報添付方法であって、

前記画像の特徴値は、当該画像のサイズであることを特徴とする画像への情報添付方法。

【請求項3】請求項1記載の画像への情報添付方法であって、

前記画像の特徴値は、当該画像全体の輝度値もしくは色値の平均値であることを特徴とする画像への情報添付方法。

【請求項4】請求項1記載の画像への情報添付方法であって、

前記画像の特徴値は、当該画像全体の輝度値もしくは色値のコントラスト値であることを特徴とする画像への情報添付方法。

【請求項5】画像情報に非画像情報を添付する、画像への情報添付方法であって、

画像情報と当該画像情報に添付すべき非画像情報とを入力するステップと、

前記入力した画像情報の表す画像中において、背景をなす領域を判別するステップと、

前記入力した画像情報を、前記判別した背景をなす領域の画像パターンが、前記入力した非画像情報の値と所定の規則とに応じて定まる画像パターンとなるように変更するステップと、を有することを特徴とする画像への情報添付方法。

【請求項6】画像情報に非画像情報を添付する、画像への情報添付方法であって、

画像情報と当該画像情報に添付すべき非画像情報とを入力するステップと、

前記入力した非画像情報の値と所定の規則とに応じて定まる画像パターンを含む画像を表す他の画像情報を生成するステップと、

前記画像情報に、前記生成した他の画像情報を添付するステップと、を有することを特徴とする画像への情報添付方法。

【請求項7】請求項1、2、3、4、5または6記載の画像への情報添付方法であって、

前記非画像情報として、前記画像情報に関連する所定の情報を、所定の前記画像情報の関係者の公開鍵暗号技術に従った秘密鍵で暗号化した電子署名を生成するステップを、さらに有することを特徴とする画像への情報添付

方法。

【請求項8】非画像情報が添付された画像情報から当該非画像情報を抽出する、画像からの情報抽出方法であって、

画像情報を入力するステップと、

前記入力した画像情報が表す画像の特徴値を求めるステップと、

前記求めた画像の特徴値と所定の規則とに従って定まる値を、前記入力した画像情報に添付された非画像情報として抽出するステップと、を有することを特徴とする画像からの情報抽出方法。

【請求項9】請求項8記載の画像からの情報抽出方法であって、

前記画像の特徴値は、当該画像のサイズであることを特徴とする画像からの情報抽出方法。

【請求項10】請求項8記載の画像からの情報抽出方法であって、

前記画像の特徴値は、当該画像全体の輝度値もしくは色値の平均値であることを特徴とする画像からの情報抽出方法。

【請求項11】請求項8記載の画像からの情報抽出方法であって、

前記画像の特徴値は、当該画像全体の輝度値もしくは色値のコントラスト値であることを特徴とする画像からの情報抽出方法。

【請求項12】非画像情報が添付された画像情報から当該非画像情報を抽出する、画像からの情報抽出方法であって、

画像情報を入力するステップと、

前記入力した画像情報の表す画像中において、背景をなす領域を判別するステップと、

前記入力した画像情報から、前記判別した領域に含まれる画像パターンを抽出するステップと、

前記抽出した画像パターンと所定の規則とに従って定まる値を、前記入力した画像情報に添付された非画像情報として抽出するステップと、を有することを特徴とする画像からの情報抽出方法。

【請求項13】非画像情報が添付された画像情報から当該非画像情報を抽出する、画像からの情報抽出方法であって、

画像情報と当該画像情報に添付された他の画像情報とを入力するステップと、

前記入力した他の画像情報と所定の規則とに応じて定まる値を、前記入力した画像情報に添付された非画像情報として抽出するステップと、を有することを特徴とする画像からの情報抽出方法。

【請求項14】画像情報に非画像情報を添付するためのプログラムが記録された記録媒体であって、

当該プログラムは、情報処理装置に、画像情報と当該画像情報に添付すべき非画像情報とを入

力するステップと、

前記入力した画像情報を、当該画像情報が表す画像の特徴値が、前記入力した非画像情報の値と所定の規則とに応じて定まる値となるように変更するステップと、を実行させることを特徴とするプログラムが記録された記録媒体。

【請求項15】画像情報に非画像情報を添付するためのプログラムが記録された記録媒体であって、当該プログラムは、情報処理装置に、画像情報と当該画像情報に添付すべき非画像情報とを入力するステップと、前記入力した画像情報の表す画像中において、背景をなす領域を判別するステップと、前記入力した画像情報を、前記判別した背景をなす領域の画像パターンが、前記入力した非画像情報の値と所定の規則とに応じて定まる画像パターンとなるように変更するステップと、を実行させることを特徴とするプログラムが記録された記録媒体。

【請求項16】画像情報に非画像情報を添付するためのプログラムが記録された記録媒体であって、当該プログラムは、情報処理装置に、画像情報と当該画像情報に添付すべき非画像情報とを入力するステップと、前記入力した非画像情報の値と所定の規則とに応じて定まる画像パターンを含む画像を表す他の画像情報を生成するステップと、前記画像情報に、前記生成した他の画像情報を添付するステップと、を実行させることを特徴とするプログラムが記録された記録媒体。

【請求項17】非画像情報が添付された画像情報から当該非画像情報を抽出するためのプログラムが記録された記録媒体であって、当該プログラムは、情報処理装置に、画像情報を入力するステップと、前記入力した画像情報が表す画像の特徴値を求めるステップと、前記求めた画像の特徴値と所定の規則とに従って定まる値を、前記入力した画像情報に添付された非画像情報として抽出するステップと、を実行させることを特徴とするプログラムが記録された記録媒体。

【請求項18】非画像情報が添付された画像情報から当該非画像情報を抽出するためのプログラムが記録された記録媒体であって、当該プログラムは、情報処理装置に、画像情報を入力するステップと、前記入力した画像情報の表す画像中において、背景をなす領域を判別するステップと、前記入力した画像情報から、前記判別した領域に含まれる画像パターンを抽出するステップと、前記抽出した画像パターンと所定の規則とに従って定ま

る値を、前記入力した画像情報に添付された非画像情報として抽出するステップと、を実行させることを特徴とするプログラムが記録された記録媒体。

【請求項19】非画像情報が添付された画像情報から当該非画像情報を抽出するためのプログラムが記録された記録媒体であって、

当該プログラムは、情報処理装置に、画像情報と当該画像情報に添付された他の画像情報とを入力するステップと、

前記入力した他の画像情報と所定の規則とに応じて定まる値を、前記入力した画像情報に添付された非画像情報として抽出するステップと、を実行させることを特徴とするプログラムが記録された記録媒体。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】本発明は、イメージデータが表す画像の視認性を保ちながら、当該イメージデータに他のデータを添付する技術に関するものである。

【0002】

【従来の技術】イメージデータが表す画像視認性を保ちながら、当該イメージデータに他のデータを添付する技術としては、電子透かし(digital watermark)と呼ばれる技術が知られている。

【0003】この技術は、IBM SYSTEMS JOURNAL, VOL 35, NOS 3&4, 1996の313頁から336頁のTechniques for data hidingなどに記載されているように、イメージデータの著作権などの管理情報を、イメージデータ自体にイメージデータと不可分に埋め込む技術である。

【0004】この電子透かしの技術は、次のような特徴を持っている。すなわち、埋め込まれた情報は、情報を埋め込んだイメージデータが表す画像を表示した場合にも、一般的には視認されず、また、視認可能な範囲において、画像自体をほとんど変化させない。一方、埋め込まれた情報のみを正確に除去することは容易でない反面、不正確に除去すると画像の画質が著しく劣化する。また、一般的には、ある程度までは、イメージデータを圧縮した場合にも、埋め込んだ情報を復元することができる。

【0005】一方、従来より、インターネットのようなオープンなネットワークを利用する、WWW(World Wide Web)サーバプログラムとブラウザプログラムとを用いるWWWシステムが知られている。

【0006】ここで、WWWシステムは、情報を公開するためのWWWサーバプログラムが動作する少なくとも一つのWWWサーバと、当該公開情報を閲覧するためのブラウザプログラムが動作する少なくとも一つのクライアント端末と、からなるシステムである。WWWサーバとクライアント端末との間で、HTTP(Hyper Text Transfer Protocol)と呼ばれる通信プロトコルにより、データのやり取りを行う。

【0007】WWWサーバで情報を公開する場合、まず、当該サーバに格納された公開すべきテキストデータ、イメージデータ、オーディオデータ、ビデオデータ、あるいは、他のWebページへのハイパーリンクデータなどを、HTML (Hyper Text Markup Language) と呼ばれる構造記述言語を用いて、相互に関連付けて一纏めにしたWebページを作成する。次に、このWebページを、他のコンピュータ（クライアント端末や他のWWWサーバ）からアクセス可能な状態で、WWWサーバの任意の格納場所（ディレクトリ）に保管する。

【0008】一方、公開されたWebページを、ユーザがクライアント端末からブラウザプログラムを用いて閲覧する場合、クライアント端末を利用するユーザがブラウザプログラムに対して、上記WebページのURL

(Universal Resource Locator) を指定すると、そのWebページのデータが、WWWサーバよりクライアント端末に送られる。そして、そのWebページに含まれるテキストデータ、イメージデータ、ビデオデータなどがクライアント端末の画面上に表示される。また、オーディオデータが、当該クライアント端末に接続されたスピーカーなどから出力される。

【0009】ところで、近年では、このようなWWWシステムをビジネスに利用しようという動きが顕著である。たとえば、WWWシステムにより商品情報を公開するいわゆる電子商取引システムなどは、そのようなビジネス利用の代表例である。

【0010】このような電子商取引システムでは、販売者は、自己のWebページに利用可能なクレジットカード会社のロゴマークなどのイメージデータを含め、消費者が支払方法を一目で認識できるようにすることが多い。これは、現実世界（インターネットのような仮想な世界ではない）において、各販売店（クレジットカード会社の加盟店）に、そこで使用可能なクレジットカードのロゴマークを掲示するのに相当する。

【0011】また、この他、Webページの発信者を示すロゴマークや、そのWebページを承認した何らかの権限ある個人／機関を示すロゴマークなどのイメージデータを、Webページに含め、Webページの利用者が、一目で、Webページの発信者やWebページが権限ある個人／機関に承認されていることを認識できるようにすることもある。

【0012】また、従来、電子データと個人／機関との関係を認証可能とする技術として、電子署名と呼ばれる技術が知られている。

【0013】電子署名は、電子データの真正さを保証するための技術であり、公開鍵暗号技術と一方向性関数を組み合わせたものである。

【0014】この技術では、まず、 $g(f(n, S), V) = n$  と、 $f(g(n, V), S) = n$  とが成立する秘密鍵S、公開鍵Vの組を作成する。ここで、nは任意の

データ、f、gは所定の関数であり、上記式は、秘密鍵Sを用いて暗号化した任意のデータは公開鍵Vを用いて復号化することができ、また、逆に、公開鍵Vを用いて暗号化した任意のデータは秘密鍵Sで復号化できることを表している。また、ここで、公開鍵Vから秘密鍵Sを求めることは実質的に不可能となっている。

【0015】秘密鍵S、公開鍵Vを作成したならば、作成者は公開鍵Vを、相手方に渡し、秘密鍵Sは作成者が秘密に保持する。

【0016】そして、鍵の作成者が、相手方にデータを送る場合には、データを所定の一方方向関数で評価した評価値を秘密鍵Sで暗号化した電子署名を、データに添付して相手方に渡す。

【0017】ここで、一方方向関数は、実質上、データから関数で評価した評価値を算出可能であるが、評価値から元のデータを算出することは実質的に不可能である性質をもつ。また、この電子署名で用いる一方方向関数には、実質的に異なるデータに対して異なるビット列を返す関数であること、すなわち、異なるデータに対して同じビット列を返す確率が極めて低い関数であること必要となる。このような関数としては、データの評価値として所定のビット列を返す一方方向ハッシュ関数などが知られている。ここで一方方向ハッシュ関数をhで表した場合、データDの一方方向ハッシュ関数による評価値h(D)をDのハッシュ値と呼ぶ。

【0018】さて、電子署名が添付されたデータを受け取った相手方は、データを一方方向関数で評価して評価値を求め、この評価値が、電子署名を公開鍵Vを用いて復号化した値と一致するかを検証する。そして、一致した場合には、電子署名が公開鍵Vに対応する秘密鍵Sの保持者によって成されたものであり、かつ、その電子署名の対象が受け取ったデータであることを認証する。

【0019】

【発明が解決しようとする課題】前記電子透かしの技術によれば、イメージデータの画像サイズに、イメージデータが表す画像の視認性を保ちながら埋め込める情報量が依存するため、画像サイズの小さなイメージデータに多くの情報を埋め込むことができないという問題がある。

【0020】このため、たとえば、前述したWebページ上のロゴマークのような小さな画像サイズのイメージデータには、わずかの情報しか埋め込むことができない。

【0021】一方、Webページ上にロゴマークをイメージデータとして含める技術によれば、ロゴマークが単なるイメージデータであるため、ロゴマークが示す個人／機関との関係をWebページが真に有しているのかどうかを認証することができないという問題がある。

【0022】このため、たとえば、前記クレジット会社のロゴマークを例にとれば、不正者が、当該クレジット

カード会社の正規加盟店のWebページから当該ロゴマークをコピーし、自己の販売店のWebページの適当な個所に当該ロゴマークを貼り付けてから、該Webページを他のコンピュータからアクセス可能な状態で、WWWサーバの任意の格納場所に保管した場合、消費者は、不正者のWebページに含まれる上記クレジットカード会社のロゴマークを見て、その不正者が正規の加盟店であるものと判断し、自己のクレジットカード番号など決済に必要なデータを当該WWWサーバに送信してしまう可能性がある。結果、不正者は、入手した消費者のクレジットカード番号を不正に入手し不正な利益を得ることが可能となる。

【0023】そこで、本発明は、イメージデータが表す画像の視認性がある程度保ちながら、イメージデータに情報を添付する新たな手法を提供することを課題とする。

【0024】また、本発明は、Webページ上のロゴマークなどの小さい画像サイズのイメージデータにイメージデータが表す画像の視認性がある程度保ちながら添付した情報によって、そのイメージデータに関連する事項の真正さを認証可能とすることを課題とする。

【0025】

【課題を解決するための手段】前記課題達成のために、本発明は、画像情報に非画像情報を添付する、画像への情報添付方法であって、画像情報と当該画像情報に添付すべき非画像情報とを入力するステップと、前記入力した画像情報を、当該画像情報が表す画像の特徴値が、前記入力した非画像情報の値と所定の規則とに応じて定まる値となるように変更するステップと、を有することを特徴とする。

【0026】ここで、画像の特徴値としては、たとえば、当該画像のサイズや、当該画像全体の輝度値もしくは色値の平均値、あるいは、当該画像全体の輝度値もしくは色値のコントラスト値などの統計的特徴値などが考えられる。

【0027】本発明では、画像の特徴値の変更によって非画像情報を画像情報へ添付する。このような方法によれば、画像の特徴値の変更の度合いが、画像情報が表す画像の視認性がある程度確保できるレベル以下となるようにすることにより、画像情報が表す画像の視認性も確保しながら、非画像情報を画像情報へ添付することが可能となる。

【0028】なお、このようにして添付された非画像情報を画像情報から抽出するには、当該画像情報が表す画像の特徴値を求め、前記求めた画像の特徴値と所定の規則とに従って定まる値を、当該画像情報に添付された非画像情報として抽出すればよい。

【0029】また、本発明の他の態様は、画像情報に非画像情報を添付する、画像への情報添付方法であって、画像情報と当該画像情報に添付すべき非画像情報とを入

力するステップと、前記入力した画像情報の表す画像中において、背景をなす領域を判別するステップと、前記入力した画像情報を、前記判別した背景をなす領域の画像パターンが、前記入力した非画像情報の値と所定の規則とに応じて定まる画像パターンとなるように変更するステップと、を有することを特徴とする。

【0030】この態様では、画像の背景領域の画像パターンの変更によって非画像情報を画像情報へ添付する。このような方法によれば、画像の背景領域における画像パターンの変更の度合いが、画像情報が表す画像の視認性がある程度確保できるレベル以下となるようにすることにより、画像情報が表す画像の視認性も確保しながら、非画像情報を画像情報へ添付することが可能となる。

【0031】なお、このようにして添付された非画像情報を画像情報から抽出するには、当該画像情報が表す画像中において背景をなす領域を判別し、判別した領域に含まれる画像パターンを当該画像情報が表す画像から抽出し、そして、抽出した画像パターンと所定の規則とに従って定まる値を、当該画像情報に添付された非画像情報として抽出すればよい。

【0032】また、本発明のさらに他の態様は、画像情報に非画像情報を添付する、画像への情報添付方法であって、画像情報と当該画像情報に添付すべき非画像情報とを入力するステップと、前記入力した非画像情報の値と所定の規則とに応じて定まる画像パターンを含む画像を表す他の画像情報を生成するステップと、前記画像情報に、前記生成した他の画像情報を添付するステップと、を有することを特徴とする。

【0033】この態様では、画像情報に、非画像情報により特定される画像パターンを有する他の画像情報を添付することにより、非画像情報を画像情報へ添付する。このような方法によれば、非画像情報の添付対象である画像情報が表す画像の視認性に影響を与えることなく、非画像情報を画像情報へ添付することが可能となる。

【0034】なお、このようにして添付された非画像情報を画像情報から抽出するには、当該画像情報に添付された他の画像情報と所定の規則とに応じて定まる値を、当該画像情報に添付された非画像情報として抽出すればよい。

【0035】なお、上記の各態様において、画像情報に添付すべき非画像情報として、当該画像情報に関連する所定の情報を、当該画像情報の関係者の公開鍵暗号法に従った秘密鍵で暗号化した電子署名を用いれば、画像情報と、当該画像情報に関連する所定の情報と、当該画像情報の関係者との関係の真正さを認証可能とすることができる。

【0036】

【発明の実施の形態】以下、本発明の実施形態を、WWWシステムにおいてWebページに貼り付けるロゴマー

クなどの図形マークに情報を埋め込む場合への適用を例にとり説明する。

【0037】まず、第1の実施形態について説明する。

【0038】図1に、本第1実施形態に係るWWWシステムの構成を示す。

【0039】図示するように、本第1実施形態に係るWWWシステムは、Webページであるコンテンツを配布するサーバ側装置100と、Webページをブラウズする通常複数のクライアント側装置200より構成される。

【0040】サーバ側装置100とクライアント側装置200の間のWebページや、その他の情報のやりとりは、ネットワーク10を介して行われる。

【0041】図2に、サーバ側装置100の構成を示す。

【0042】図示するように、サーバ側装置100は、処理部110と記憶部120よりなる。また、処理部110は、各種入出力を担う入出力部111、サーバ側装置100内の各部の制御を行う制御部112、認証用の情報などの図形マークに埋め込む情報である挿入情報122を生成する情報生成部113、図形マークに情報を埋め込む情報挿入部114、情報を埋め込んだ図形マークをWebページに貼り付けるマーク貼付部115、および、Webページをネットワーク上に公開するWebサーバ部116よりなる。また、記憶部120は、図形マーク122を貼り付ける前のWebページであるオリジナルコンテンツ121、図形マークに埋め込む情報である挿入情報122、情報を埋め込む図形マーク123、情報を埋め込んだ図形マーク124、および、情報を埋め込んだ図形マークを貼付したWebページであるマーク添付コンテンツ125を記憶する。Webサーバ部116は、このマーク添付コンテンツ125をネットワーク10上に公開する。

【0043】次に、図3にクライアント側装置200の構成を示す。

【0044】図示するように、クライアント側装置200は、処理部210と記憶部220よりなる。また、処理部210は、各種入出力を担う入出力部211、クライアント側装置200内の各部の制御を行う制御部212、および、ネットワーク上のWebサーバよりWebページを取り込み出力するブラウザ部213を備えている。また、処理部210は、ブラウザ部213が取り込んだWebページが、マーク添付コンテンツ221である場合に、マーク添付コンテンツ221から情報入り図形マーク222を切り出す情報入りマーク切り出し部214、情報入り図形マーク222から挿入情報223を抽出する情報抽出部215、および、挿入情報223を用いて認証処理を行う認証部216を備えている。

【0045】記憶部220は、マーク添付コンテンツ221、情報入り図形マーク222、挿入情報223、認

証処理に用いる公開鍵情報224、図形マーク225などを記憶している。

【0046】ここで、サーバ側装置100やクライアント側装置200は、図4に示すように、CPU301や、主記憶302、ハードディスク装置である外部記憶装置303b、他の外部記憶装置である303a、通信制御装置304、キーボードやポインティングデバイスなどの入力装置305、表示装置などの出力装置306などを備えた、一般的な構成を有する電子計算機上に構築することができる。

【0047】この場合、サーバ側装置100の処理部110、および、処理部110の内部の各部は、CPU301が主記憶302にロードされたプログラムを、適当なOS上で実行することにより電子計算機上に具現化されるプロセスとして実現される。また、この場合、主記憶302や外部記憶装置303a、bが、サーバ側装置100の記憶部120として使用される。また、同様に、クライアント側装置200の処理部210、および、処理部210の内部の各部は、CPU301が主記憶302にロードされたプログラムを実行することにより電子計算機上に具現化されるプロセスとして実現される。また、この場合、主記憶302や外部記憶装置303が、クライアント側装置200の記憶部220として使用される。

【0048】前述した主記憶302にロードされCPU301によって実行されることにより、電子計算機上にサーバ側装置100とクライアント側装置200を構成するためのプログラムは、予め、外部記憶装置303bに記憶され、必要に応じて主記憶302にロードされ、CPU301によって実行される。または、可搬型の記憶媒体307、たとえば、CD-ROMを扱う外部記憶装置303aを介して、直接、必要に応じて、可搬型の記憶媒体307から主記憶302にロードされ、CPU301によって実行される。もしくは、一旦、可搬型の記憶媒体を扱う外部記憶装置303aを介して、可搬型の記憶媒体307から、ハードディスク装置などの外部記憶装置303b上にインストールされた後、必要に応じて主記憶302にロードされ、CPU301によって実行される。

【0049】以下、サーバ側装置100とクライアント側装置200の行う処理の詳細を説明する。

【0050】まず、サーバ側装置100の行う処理について説明する。

【0051】制御部112は、入出力部111とから、オリジナルコンテンツ121と、オリジナルコンテンツ121に貼り付ける図形マーク123を受け入れ、一旦、記憶部120に記憶する。一方、情報生成部113は、図形マークに埋め込む挿入情報123を生成し、記憶部120に記憶する。

【0052】ここで、情報生成部113は、図形マーク

に埋め込む挿入情報123として、図形マークによって認証可能とする事項を認証するために必要な情報を生成する。たとえば、図形マークがロゴマークであり、そのロゴマークの真正さを認証可能とするのであれば、情報生成部113は、図形マーク123のハッシュ値を、その真正さを認める権威ある権威者や適当な第三者機関の秘密鍵で暗号化した電子署名を挿入情報123として生成する。この秘密鍵は、あらかじめ記憶部120に記憶しておき、これを情報生成部113が読み込むようにする。

【0053】また、たとえば、図形マークがロゴマークであり、そのロゴマークと、そのロゴマークが貼り付けられたオリジナルコンテンツ121との関係の真正さを認証可能とするのであれば、オリジナルコンテンツ121のハッシュ値を、その真正さを認める権威ある権威者や適当な第三者機関の秘密鍵で暗号化した電子署名を挿入情報123として生成する。

【0054】また、たとえば、図形マークがロゴマークであり、そのロゴマークの真正さと、そのロゴマークと、そのロゴマークが貼り付けられたオリジナルコンテンツ121との関係の真正さを認証可能とするのであれば、図形マーク123のハッシュ値と、オリジナルコンテンツ121のハッシュ値とを、それぞれ、その真正さを認める権威ある権威者や適当な第三者機関の秘密鍵で暗号化した電子署名を挿入情報123として生成する。

【0055】または、これら以外の、認証可能とする真正さを認証するために必要な情報や、その他所望の情報、たとえば、日付情報などを含めた情報を挿入情報123として生成する。なお、サーバ側装置100の利用者と、認証可能とする真正さを認める権威ある権威者や適当な第三者機関が異なる場合には、情報生成部113は権威者や適当な第三者機関の秘密鍵を知ることができないので、この場合は、入出力装置を介して権威者や適当な第三者機関側と情報をやりとりし、権威者や適当な第三者機関側に、権威者や適当な第三者機関の秘密鍵を用いた暗号化の依頼を、暗号化に必要な情報と共に送り、その応答として権威者や適当な第三者機関から送られた挿入情報を記憶部120に格納する。ここで、このような権威者や適当な第三者機関側と情報をやりとりは、もちろん、ネットワーク10を介して行うようにしてよい。

【0056】次に、情報挿入部114は、図形マーク123に、挿入情報122を埋め込む埋め込み処理を行う。

【0057】図5に、この埋め込み処理の処理手順を示す。

【0058】以下、その詳細を、図形マーク123が $128 \times 128$ 画素の画像であり、各画素は、一つの輝度データと2つの色差データから構成され、挿入情報122が55ビットの情報である場合を例にとり説明する。

【0059】さて、埋め込み処理では、まず、挿入情報122を、各5ビットの7つのビット列と、20ビットのビット列の8つのビット列に分割する。

【0060】そして、まず、最初の5ビットのビット列を、サイズによる埋め込み（ステップ801）によって図形マーク123に埋め込む。このサイズによる埋め込みでは、図形マーク123の画像サイズを、縦横それぞれの画素数が、 $32 \times n + a$ になるように変更する。ここで、 $a$ は、埋め込む5ビットのビット列が表す10進数であり、 $n$ は、 $32 \times n + a$ を、最も図形マーク123の元の画像サイズ（この場合は128）に近くする数値である。

【0061】なお、このような画像サイズの変更は、図形マーク123の拡大、縮小によって行ってもよいし、たとえば、変更後に画素値が増加するような場合には、特定色（たとえば白）の画素を付加することにより行ってもよい。

【0062】このようにすることにより、図形マーク123の画像サイズは、5ビットの値によって、縦横それぞれについて115画素から146画素に変更することになる。したがって、このサイズによる埋め込みによる図形マーク123の画像サイズの変更の程度は、縦横それぞれについて10数パーセント程度であるので、図形マーク123の視認性が大きく失われることはない。

【0063】次に、次の5ビットのビット列を、輝度シフトによる埋め込み（ステップ802）によって図形マーク123に埋め込む。この輝度シフトによる埋め込みでは、図形マーク123の各輝度データを、その図形マーク123の全体の輝度データの平均値が $32 \times n + a$ になるように変更する。ここで、 $a$ は、埋め込む5ビットのビット列が表す10進数であり、 $n$ は、 $32 \times n + a$ を、図形マーク123全体の元の輝度データの平均値に最も近くする数値である。

【0064】次に、次の5ビットのビット列を、輝度コントラストによる埋め込み（ステップ803）によって図形マーク123に埋め込む。この輝度コントラストによる埋め込みでは、図形マーク123の各輝度データを、その図形マーク123の輝度コントラストが、 $32 \times n + a$ になるように変更する。ここで、 $a$ は、埋め込む5ビットのビット列が表す10進数であり、 $n$ は、 $32 \times n + a$ を、最も図形マーク123全体の元の輝度コントラストに近くする数値である。ここで、図形マーク123の全体の輝度コントラストは、図形マーク123全ての輝度データの標準偏差とする。

【0065】以下、残りの二つの色差データについても、各々5ビットのビット列についての、色差シフトによる埋め込み（ステップ804、806）と、色差コントラストシフトによる埋め込み（ステップ805、807）を、輝度データと同様にして行う。

【0066】そして、最後に、残った10ビットを電子



透かしによって図形マーク123に埋め込み(ステップ808)、情報入り図形マーク124として記憶部120に格納する。

【0067】ただし、以上のステップ801から807による情報の埋め込みは、全てを行う必要がない。埋め込みによる図形マークの視認性の劣化や、埋め込むべき情報のビット数に応じて、一部のみを実行したり、各ステップにおいて埋め込む情報のビット数を異ならせるようにする。また、輝度、色差表現の代わりにRGBなどを画素値の表現用い、各色の平均値やコントラストとして情報を埋め込むようにしてもよい。

【0068】また、ステップ808における電子透かしによる埋め込みを行う情報のビット数は、その埋め込みによって、輝度/色差の平均値や、輝度/色差コントラストのうち、情報の埋め込みに用いた値を整数に丸めた値を変化させない程度に押さえるようにする。

【0069】以上のような処理によって、図形マークの視認性を保ちながら、従来の電子透かしのみによって情報を埋め込む場合に比べ、より多くのデータを埋め込むことが可能となる。

【0070】さて、図2に戻り、マーク添付部115は、記憶部120に格納されたオリジナルコンテンツ121を編集し、情報入り図形マークを貼り付け、マーク添付コンテンツ125を作成し、記憶部120に格納する。オリジナルコンテンツ121への、情報入り図形マークを貼り付けは、具体的には、オリジナルコンテンツ121がHTML文書である場合には、HTML文書中に、情報入り図形マークファイルの場所(URL)を<IMG SRC>タグを用いて記述することにより行う。

【0071】WWWサーバ部116は、Webページであるマーク添付コンテンツ125をネットワーク10に公開する。

【0072】以上、サーバ側装置100が行う処理について説明した。

【0073】以下、クライアント側装置200の行う処理について説明する。

【0074】ブラウザ部13は、ネットワーク上のWebサーバよりWebページを取り込み、記憶部220に記憶すると共に、その内容を入出力部211よりユーザに出力する。

【0075】情報入りマーク切り出し部214は、記憶部220に記憶されたWebページが、マーク添付コンテンツ125である場合に、入出力部211を介して認証処理を指示されると、マーク添付コンテンツ221より情報入り図形マーク222を切り出し、記憶部220に記憶する。情報抽出部215は、情報入り図形マーク222に埋め込まれた挿入情報223を復元し、記憶部220に記憶する。

【0076】この情報抽出部215が行う挿入情報を復元する処理の手順を図6に示す。

【0077】図示するように、この処理では、まず、情報入り図形マーク222の縦、横の画素数を求め、これを32で割った値の余りを5ビットで表現した値を、5ビットの情報として復元する(ステップ901)。

【0078】次に、情報入り図形マーク222全体の輝度データの平均値を求め、平均値を32で割った値の余りを5ビットで表現した値を復元する(ステップ902)。

【0079】そして、情報入り図形マーク222全体の輝度データのコントラストを求め、コントラスト値を32で割った値の余りを5ビットで表現した値を復元する(ステップ903)。

【0080】また、同様に、色差データ1、色差データ2についても、それぞれ、その平均値とコントラストより、5ビットづつ情報を復元する(ステップ904~907)。

【0081】そして、最後に、情報入り図形マーク222に埋め込まれた電子透かしを従来と同様に抽出し、これより10ビットを復元する(ステップ901)。

【0082】そして、以上で求めた各ビットを連結し、45ビットの情報を復元し、処理を終了する。

【0083】さて、図3に戻り、認証部216は、挿入情報223が認証可能としている事項の認証を行う。

【0084】たとえば、図形マークがロゴマークであり、そのロゴマークの真正さを認証するのであれば、認証部216は、オリジナル図形マーク225のハッシュ値を求め、これと、挿入情報223を真正さを認める権威ある権威者や適当な第三者機関の公開鍵情報224で復号した値と比較し、一致した場合に、真正さを認証する。ここで、オリジナル図形マーク225は、このWebページを公開したサーバ側装置100が正当なものであれば、サーバ側装置100の図形マーク123と同じものであり、情報が埋め込まれる前の情報入り図形マーク222に相当する。

【0085】ここで、オリジナル図形マーク225と公開鍵情報224は、別途、真正さを認める権威ある権威者や適当な第三者機関より別途信頼できる方法でブラウザ部213または入出力部211を介して入手し記憶部220に記憶する。

【0086】また、たとえば、図形マークがロゴマークであり、そのロゴマークと、そのロゴマークが貼り付けられたオリジナルコンテンツ121との関係の真正さするのであれば、マーク添付コンテンツ221から、情報入り図形マーク222を除いたオリジナルコンテンツを復元し、そのハッシュ値を求め、これと、挿入情報223を真正さを認める権威ある権威者や適当な第三者機関の公開鍵情報224で復号した値と比較し、一致した場合に、真正さを認証する。

【0087】また、たとえば、図形マークがロゴマーク

であり、そのロゴマークの真正さと、そのロゴマークと、そのロゴマークが貼り付けられたオリジナルコンテンツ121との関係の真正さを認証可能とするのであれば、オリジナル図形マーク225のハッシュ値と、マーク添付コンテンツ221から、情報入り図例マーク222を除いたオリジナルコンテンツのハッシュ値とを求め、これと、挿入情報223を真正さを認める権威ある権威者や適当な第三者機関の公開鍵情報224で復号した値と比較し、一致した場合に、真正さを認証する。

【0088】そして、認証部216は、認証した結果を出力部211を介してユーザに通知する。

【0089】ところで、以上のような認証処理は、ネットワーク10上に信頼できる認証装置を設け、クライアント側装置200の認証部216が、この認証装置と協調して行うようにしてもよい。

【0090】たとえば、予め、認証装置に、オリジナルコンテンツやオリジナル図形マークや権威者や適当な第三者機関の公開鍵情報のうちのいずれかもしくは全てを登録しておくようにする。そして、認証時には、クライアント側装置200の認証部216が挿入情報や、その他の認証処理に必要な情報を認証装置にネットワーク10介してを送り、認証装置が前述したような認証処理を行い、その結果をクライアント側装置200の認証部216に返すようにする。

【0091】なお、本実施形態に係るクライアント側装置200の、情報入りマーク切り出し部214、情報抽出部215、認証部216は、ブラウザプログラムにより実現されるブラウザ部213に対するプラグインソフトウェアによって実現するようにしてもよい。また、この場合は、ブラウザ部213が行うマーク添付コンテンツの表示上で、情報入り図形マークがユーザによって選択されたときに、情報入りマーク切り出し部214、情報抽出部215、認証部216を実現するプラグインソフトウェアを起動し、前述した情報入りマーク切り出し部214、情報抽出部215、認証部216に選択された情報入り図形マークについての前述した処理を行わせるようにするのがよい。ただし、この場合には、情報入り図形マークのデータファイルには特別な拡張子などを与えることなどにより、ブラウザ部213が、この情報入り図形マークが、このようなプラグインソフトウェアによって処理されるべきものであることを認識できるようにする。

【0092】また、本実施形態に係るサーバ側装置100に、オリジナルコンテンツ121を生成、編集するエディタプログラムの実行によって実現されるエディタ部を備えるようにしてもよい。そして、この場合、前述した情報生成部113、情報挿入部114、マーク貼付部115は、エディタプログラムから利用可能なプラグインソフトウェアとして実現するようにしてもよい。この場合、このプラグインソフトウェアは、エディタプロ

ラムが提供するメニューの選択によって、起動され、前述の情報生成部113、情報挿入部114、マーク貼付部115の処理を実行することによって、エディタプログラムが編集しているオリジナルコンテンツ121を編集してマーク添付コンテンツ125を生成する。

【0093】以上、第1の実施形態について説明した。

【0094】以下、第2の実施形態について説明する。

【0095】本第2実施形態は、第1実施形態と、サーバ側装置100の情報挿入部114の行う、挿入情報122の図形マーク123への埋め込み方と、クライアント側装置200の情報入りマーク切り出し部214が行う切り出しと、情報抽出部215が行う挿入情報の抽出の仕方が異なる。

【0096】第2実施形態における、情報挿入部114が行う挿入情報122について説明する。

【0097】図7に示すように、本第2実施形態では、図形マーク123に第2の画像を添付する。

【0098】第2の画像1230は、図8に示すように、たとえば、128×40画素の画像であり、4×4画素ごとに320のブロックに分割されている。情報挿入部114は、たとえば、300ビットの挿入情報122の各ビットを、320のブロック中の所定の規則に従った優先順序で選択した300ブロックの各々に割り当て、各ブロックをそのブロックに割り当てたビットの値に応じた色で塗りつぶす。たとえば、値1のビットを割り当てたブロックは黒で塗りつぶし、値0のビットを割り当てたブロックは白で塗りつぶす。そして、図形マーク123と第2の画像1230を、情報入り図形マーク124として記憶部120に格納する。

【0099】なお、以上の処理におけるブロックは1×1画素のブロック、すなわち、画素そのものとしてもよく、この場合は、第2の画像のサイズはより小さくて済む。

【0100】さて、この場合、マーク添付部115は、記憶部120に格納されたオリジナルコンテンツ121を編集し、情報入り図形マーク124として記憶部120に格納された、図形マーク123と第2の画像1230をオリジナルコンテンツ121に貼り付けて、マーク添付コンテンツ125を作成し、記憶部120に格納する。WWWサーバ部116は、Webページであるマーク添付コンテンツ125をネットワーク10に公開する。

【0101】一方、クライアント側装置300の、情報入りマーク切り出し部214は、ユーザから認証処理を指示されると、前述した第2の画像を切り出し、記憶部220に記憶する。クライアント側装置300の情報抽出部215は、所定の規則に従った優先順序で、第2の画像の320のブロック中の300ブロックを選択し、各ブロックの塗りつぶし色をビット値に変換する。たとえば、白で塗りつぶされたビットは値0のビットに、黒で

塗りつぶされたビットは値1のビットに変換する。そして、変換したビットを連結し、300ビットの挿入情報223を復元する。

【0102】次に、第3の実施形態について説明する。

【0103】本第3実施形態は、第1実施形態と、サーバ側装置100の情報挿入部114の行う、挿入情報122の図形マーク123への埋め込み方と、クライアント側装置200の情報抽出部215が行う挿入情報の抽出の仕方が異なる。

【0104】第3実施形態における、情報挿入部114が行う挿入情報122について説明する。

【0105】図9に示すように、本第2実施形態では、図形マーク123の背景部1232を、挿入情報122を埋め込んだ画像で置き換える。ここで、図形マーク123の背景部1232とは、図形マーク123中で有意な図形、文字1231を含んでいない部分を指す。図形マーク123の背景部の領域を判別する方法としてはさまざまな手法があるが、たとえば、予め、背景部の領域の画素値を特定の値として図形マーク123を作成したり、予め背景部の領域を示す情報（マスクレイヤや、 $\alpha$ チャンネルと呼ばれる情報など）を付加して図形マーク123を作成して、これら情報より背景部の領域を判別したりする手法などを用いることができる。

【0106】さて、情報挿入部114は、このようにして背景部の領域を判別したならば、その領域に含まれる、画素または所定サイズ（たとえば2×2画素）のブロックを、所定の規則に従って順次選択し、挿入情報122の各ビットを、選択した画素またはブロックの各々に順次割当て、各画素またはブロックを割り当てたビットの値に応じた色で塗りつぶす。たとえば、値1のビットを割り当てた画素またはブロックは黒で塗りつぶし、値0のビットを割り当てたブロックは白で塗りつぶす。そして、図形マーク123を、情報入り図形マーク124として記憶部120に格納する。

【0107】ただし、情報挿入部114は、このように挿入情報122のビットの値に応じて塗りつぶした画素またはブロックの領域を識別できるよう、この領域を示す情報（マスクレイヤや、 $\alpha$ チャンネルと呼ばれる情報など）を付加して図形マーク123を作成するようにしてもよい。

【0108】また、情報挿入部114は、このように挿入情報122のビットの値に応じて塗りつぶした画素またはブロックの領域を識別できるよう、挿入情報122のビットの値に応じて塗りつぶした画素またはブロックの領域の範囲を示す特定の画像パターンを図形マークに含めるようにしてもよい。たとえば、背景部の領域の画素またはブロックをラスタ順に走査した場合に、連続して走査されることになる画素またはブロックの領域の始まりと終わりの部分を特定のパターンで塗りつぶし、特定のパターンで塗りつぶした部分の間の背景部の領域の

画素またはブロックを挿入情報122のビットの値に応じた色で塗りつぶすようにする。

【0109】また、挿入情報122のビットの値に応じて塗りつぶす色を、情報入り図形マーク123のビットの値に応じて塗りつぶした画素以外の画素で使用されていない色とすることにより、挿入情報122のビットの値に応じて塗りつぶした画素またはブロックの領域を識別できるようにしてもよい。これは、たとえば、塗りつぶす色を白と黒とするならば、塗りつぶした画素以外の白または黒の画素の色を幾分変更（たとえば、白は白に近い灰色に、黒は黒に近い灰色）することにより実現することができる。

【0110】一方、クライアント側装置300の情報抽出部215は、まず、情報入り図形マーク222の背景部を前述した領域を示す情報や特定の画像パターンより識別し、その領域に含まれる、画素または所定サイズ（たとえば2×2画素）のブロックを、所定の規則に従って順次選択し、各画素またはブロックの塗りつぶし色をビット値に変換する。たとえば、白で塗りつぶされたビットは値0のビットに、黒で塗りつぶされたビットは値1のビットに変換する。そして、変換したビットを連結し、挿入情報223を復元する。

【0111】以上、本発明の実施形態について説明した。

【0112】

【発明の効果】以上のように、本発明によれば、イメージデータが表す画像の視認性のある程度保ちながら、イメージデータに情報を添付する新たな手法を提供することができる。

【0113】また、本発明は、Webページ上のロゴマークなどの小さい画像サイズのイメージデータにイメージデータが表す画像の視認性のある程度保ちながら添付した情報によって、そのイメージデータに関連する事項の真正さを認証可能とすることができる。

【図面の簡単な説明】

【図1】本発明の実施形態に係るWWWシステムの構成を示すブロック図である。

【図2】本発明の実施形態に係るサーバ側装置の構成を示すブロック図である。

【図3】本発明の実施形態に係るクライアント側装置の構成を示すブロック図である。

【図4】一般的な電子計算機の構成を示すブロック図である。

【図5】本発明の第1実施形態において行う、図形マークへ情報を埋め込む処理の手順を示すフローチャートである。

【図6】本発明の第1実施形態に係る、情報が埋め込まれた図形マークから情報を抽出する処理の手順を示すフローチャートである。

【図7】本発明の第2実施形態に係る図形マークへの情

報の添付のようすを示す図である。

【図8】本発明の第2実施形態に係る、情報を埋め込んだ画像を示す図である。

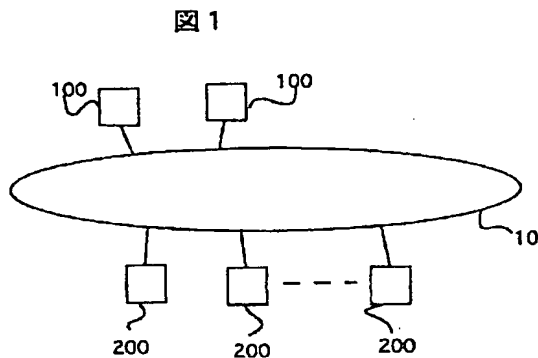
【図9】本発明の第3実施形態に係る、情報を埋め込んだ画像を示す図である。

【符号の説明】

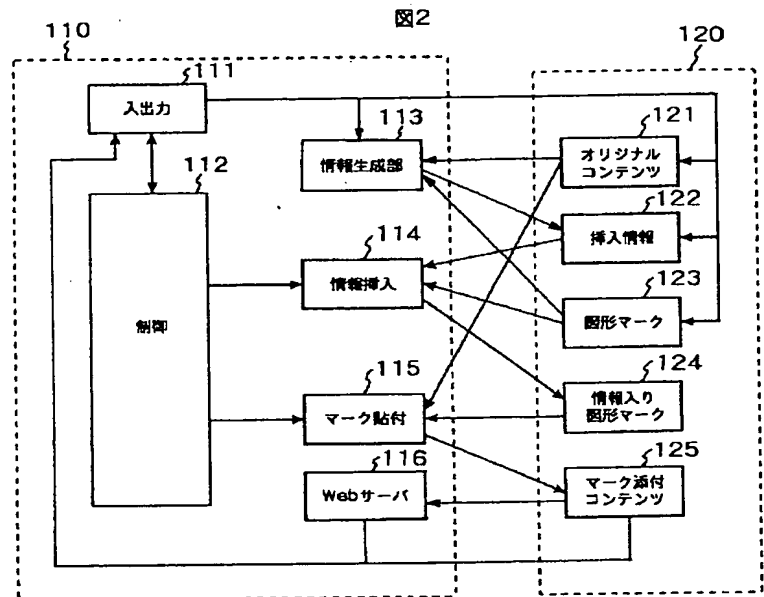
10 ネットワーク  
100 サーバ側装置  
110 処理部  
111 入出力部  
112 サーバ側装置  
113 情報生成部  
114 情報挿入部  
115 情報挿入部

115 マーク貼付部  
116 Webサーバ部  
120 記憶部  
200 クライアント側装置  
210 処理部  
220 記憶部  
211 入出力部  
212 制御部  
213 ブラウザ部  
214 情報入りマーク切り出し部  
215 報抽出部  
216 認証部  
220 記憶部

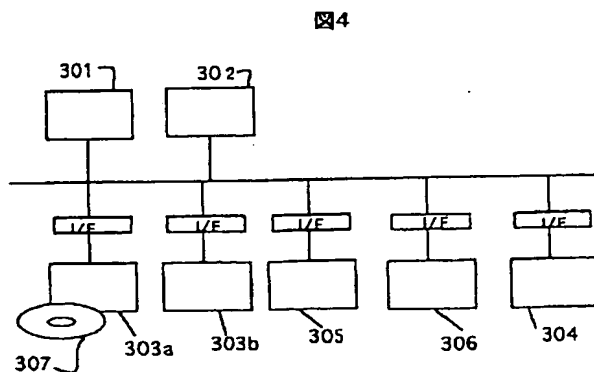
【図1】



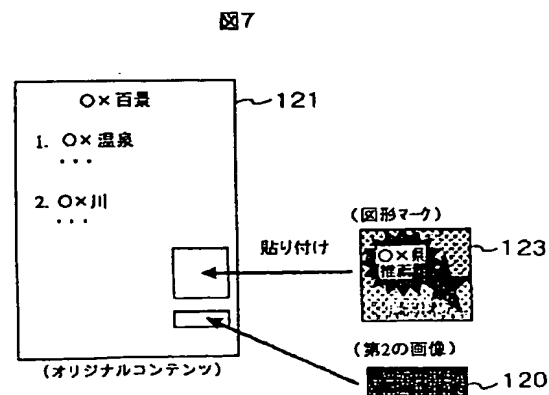
【図2】



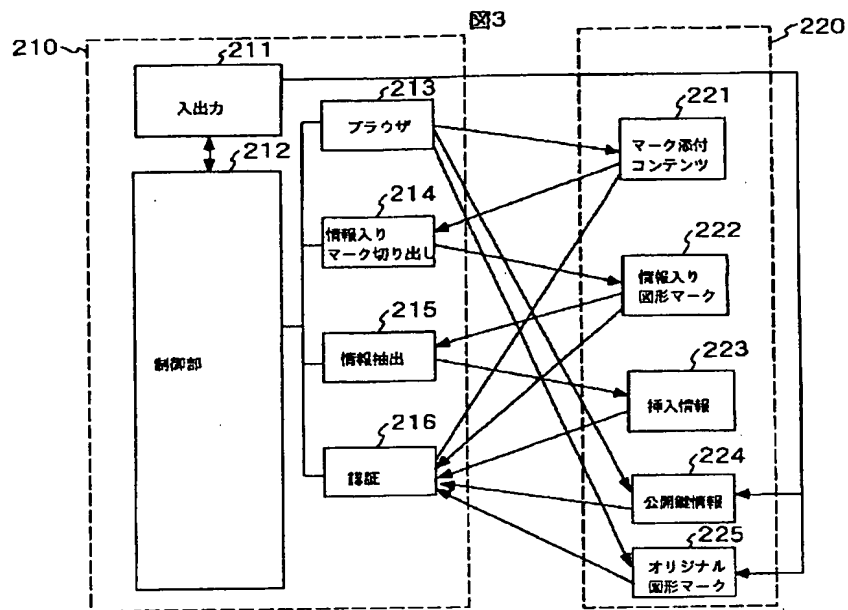
【図4】



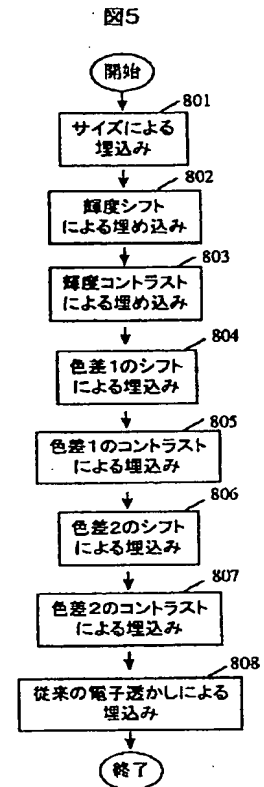
【図7】



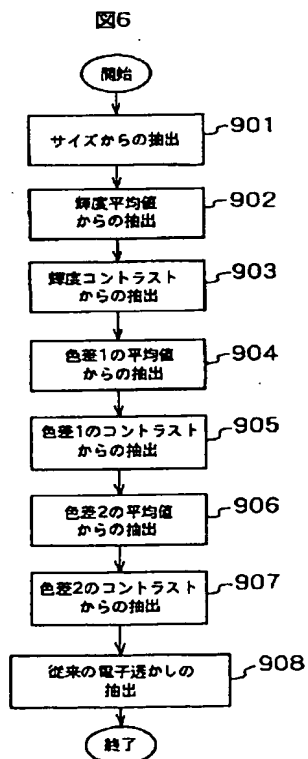
【図3】



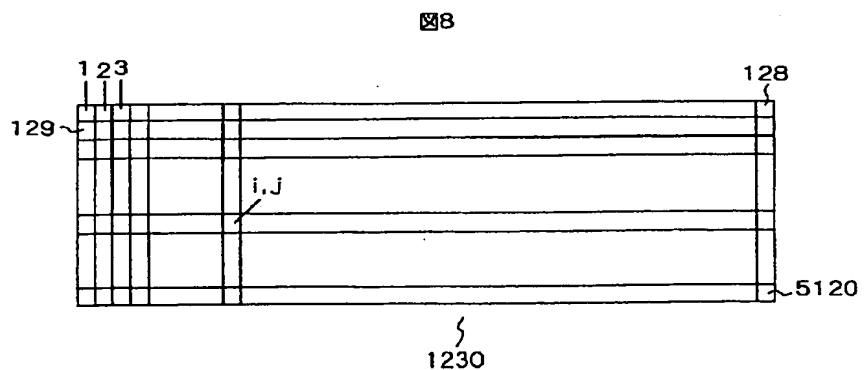
【図5】



【図6】

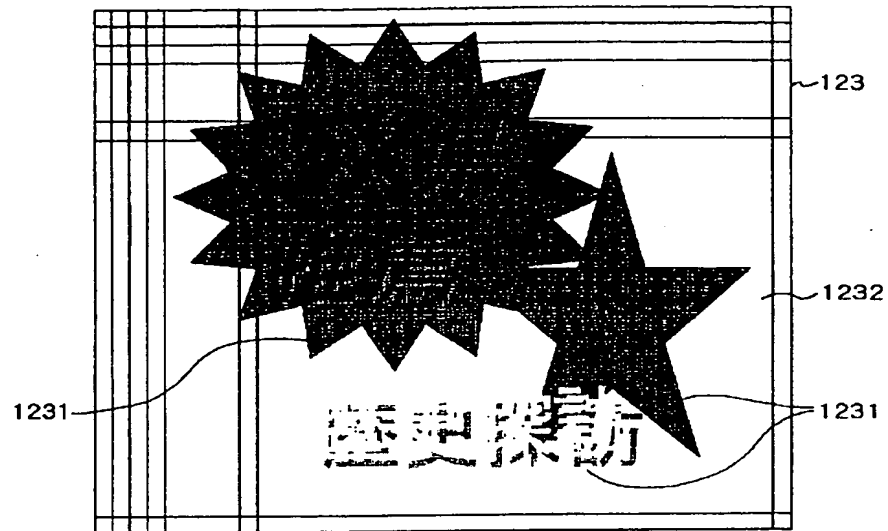


【図8】



【図9】

図9



## フロントページの続き

(72) 発明者 永井 康彦  
 神奈川県川崎市麻生区王禅寺1099番地 株  
 式会社日立製作所システム開発研究所内  
 (72) 発明者 篠田 隆志  
 東京都江東区新砂一丁目6番27号 株式会  
 社日立製作所公共情報事業部内

Fターム(参考) 5B057 AA20 CA01 CA02 CA08 CA12  
 CA16 CB01 CB02 CB08 CB12  
 CB16 CC03 CD05 CE08 CE09  
 CE11 CE17 CG07 CG09 CH01  
 CH11 DA08 DA17 DB02 DB05  
 DB06 DB09 DC02  
 5C076 AA02 AA13 AA14 AA16 AA21  
 AA22 AA40 BA06 CA10 CB02

**This Page is Inserted by IFW Indexing and Scanning  
Operations and is not part of the Official Record**

**BEST AVAILABLE IMAGES**

Defective images within this document are accurate representations of the original documents submitted by the applicant.

Defects in the images include but are not limited to the items checked:

- ☐ BLACK BORDERS
- ☐ IMAGE CUT OFF AT TOP, BOTTOM OR SIDES
- ☒ FADED TEXT OR DRAWING
- ☒ BLURRED OR ILLEGIBLE TEXT OR DRAWING
- ☐ SKEWED/SLANTED IMAGES
- ☐ COLOR OR BLACK AND WHITE PHOTOGRAPHS
- ☐ GRAY SCALE DOCUMENTS
- ☒ LINES OR MARKS ON ORIGINAL DOCUMENT
- ☐ REFERENCE(S) OR EXHIBIT(S) SUBMITTED ARE POOR QUALITY
- ☐ OTHER: \_\_\_\_\_

**IMAGES ARE BEST AVAILABLE COPY.**

**As rescanning these documents will not correct the image problems checked, please do not report these problems to the IFW Image Problem Mailbox.**